STRATEGY RESEARCH PROJECT

21ST CENTURY INFORMATION MANAGEMENT AT THE COMBATANT COMMANDER LEVEL

BY

COMMANDER JUDY M. ANDERSON
United States Navy

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

21ST CENTURY INFORMATION MANAGEMENT AT THE COMBATANT COMMANDER LEVEL

by

Commander Judy M. Anderson
United States Navy

Colonel Edward J. Filiberti
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Judy M. Anderson, Commander, United States Navy

TITLE: 21ST Century Information Management at the Combatant Commander Level

FORMAT: Strategy Research Project

DATE: 31 March 2000 PAGES: 21 CLASSIFICATION: Unclassified

Information superiority will be the key enabler for achieving Joint Vision 2010: Full Spectrum Dominance. The Department of Defense (DoD) is in the early stages of dealing with the information management challenges presented in Joint Vision 2010. There is an urgent need for the creation of a single, DoD-wide overall doctrinal concept for information management. This concept must be backed by the authority of the Chairman, Joint Chiefs of Staff, with United States Joint Forces Command the likely candidate for leading the coordination effort. In designing the overarching information management concept, it should be viewed as a cycle, similar to the Intelligence Cycle. The cycle consists of the following six phases: (1) Planning and Direction, (2) Collection, (3) Processing and Exploitation, (4) Analysis and Production, (5) Dissemination and Integration, and (6) Evaluation and Feedback.

This paper discusses the DoD's information management requirements and examines selected initiatives applicable to the combatant commander's information management requirements. A methodology for structuring information management as a cycle is developed in detail. Problem areas are highlighted and recommendations are offered for achieving Joint Vision 2010 goals.

TABLE OF CONTENTS

ABSTRACT III

21ST CENTURY INFORMATION MANAGEMENT AT THE COMBATANT COMMANDER LEVEL 1

THE INFORMATION MANAGEMENT CHALLENGE 1

THE INFORMATION CYCLE: 3

PLANNING AND DIRECTION PHASE: 4

COLLECTION PHASE: 4

PROCESSING AND EXPLOITATION PHASE: 4

ANALYSIS AND PRODUCTION PHASE: 5

DISSEMINATION AND INTEGRATION PHASE: 5

EVALUATION AND FEEDBACK PHASE: 5

A NEW PARADIGM FOR INFORMATION MANAGEMENT? 5

SECURITY AND INTEROPERABILITY ISSUES 8

THE WAY AHEAD 9

RECOMMENDATIONS 11

ENDNOTES 13

BIBLIOGRAPHY 15

21ST CENTURY INFORMATION MANAGEMENT AT THE COMBATANT COMMANDER LEVEL

Information Superiority will be the key enabler for achieving Joint Vision 2010: Full Spectrum Dominance.[1] At the Combatant Commander level, one of the most critical areas of concern for the 21st Century is information management. "The Warfighter's primary goal to enhance his decision-making capability is to have the right information arrive at the right place, at the right time, in a useable form for mission accomplishment."[2] Information management applies to all aspects of the operational environment and is critical to "information superiority", or "dominant battlespace awareness", as it is termed in Joint Vision 2010.[3] Even the most cursory review of national security and military policies surfaces the critical importance of applying emerging technology to the challenges of managing the flow of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) information in support of the warfighter's Command and Control (C2) processes.

The Department of Defense (DoD) and its components are in the early stages of dealing with the information management challenges presented in Joint Vision 2010. This paper discusses the DoD's information management requirements. It concentrates primarily on the Combatant Commander level, the current environment as it affects information management initiatives, and examines selected initiatives applicable to the Combatant Commander's information management requirements. A methodology for structuring information management within a useable cycle is developed in detail. Most importantly, the paper will highlight problem areas and offer recommendations for achieving Joint Vision 2010 goals.

THE INFORMATION MANAGEMENT CHALLENGE

It is widely accepted that, in the past decades, the United States has transitioned from the "Industrial Age" to the "Information Age". The military has been an integral part of this transformation. However, there continues to be debate about the actual impact of the Information Age on warfighting. Many analysts believe that advances in communications and computer technology, particularly within the 1990s, have caused a corresponding revolution in military affairs. Many aspects of this "revolution" deal with the management of information critical to C2. As one leading academician postulates, "Integrative technology could dramatically enhance the ability to coordinate the actions of widely dispersed and dissimilar units, establishing the "system of systems" as the dominant military architecture of the new era."[4] However, this potential will remain unrealized unless and until the relevant technology can be properly harnessed. Improperly managed information is hardly better than no information at all. It is just as likely to result in information overload, confusion, frustration, wasted effort and resources, and other negative factors than facilitate warfighting. The draft Capstone Requirements Document for Information Dissemination Management (CRD-IDM), in development by United States Joint Forces Command in response to tasking by the Vice Chairman of the Joint Chiefs of Staff[5] clearly expresses this problem:

> While creating greatly enhanced information capabilities, the explosion in information technology is simultaneously threatening the smooth flow of essential information to the

> warfighter and greatly complicating our ability to define and implement information management policies and procedures.[6]

The CRD-IDM is not alone in identifying "overload" as the primary information management problem. "Overload" currently typifies the information management environment at the Combatant Commander level. In July 1999, USCINCPAC documented its headquarter's current situation in a proposal for an Advanced Concept Technology Demonstration (ACTD) titled "CINC 21":

> During a crisis, the flood of information that becomes available is such that accessing relevant information, placing it in context, and understanding relevance is extremely difficult, and requires a high level of experience that is becoming more rare. When faced with multiple, simultaneous crises in theater, the deluge of information is even greater, and today's battle staffs are constrained by their command center spaces, display design and organizationally-limited information flow. Making information relevant means the information must be organized around mission needs, managed to insure consistency, and shared with distributed sites to be optimally useful. To further complicate the problem, the current network pipeline becomes severely constrained in capacity the farther one gets away from major headquarters elements.[7]

Nevertheless, if proper procedures are implemented and appropriate equipment is procured, it is possible to leverage the "emerging" revolution in military affairs to achieve information dominance. The resulting improvement in battlespace awareness, increased speed and effectiveness of command decision-making, and an enhanced ability to deal with complexity will provide the U.S. military advantages vastly superior to any potential adversary. Equally important, improved information management can and should result in more efficient management of all operations including humanitarian assistance, disaster relief, etc. Joint Vision 2010 clearly articulates the criticality of this capability:

> **Improvements in information and systems integration technologies will also significantly impact future military operations** by providing decision makers with accurate information in a timely manner. Information technology will improve the ability to see, prioritize, assign, and assess information. Forces harnessing the capabilities potentially available from this system of systems will gain **dominant battlespace awareness**...[emphasis in the original] [8]

Joint Vision 2010 describes itself as a "conceptual template". The military must interpret and implement that guidance by developing equipment, doctrine, training, organization, and leadership to achieve the vision. Numerous efforts--some complementary, some duplicative--are underway to address information management requirements. The overall challenge is so complex that no single initiative is addressing the entire scope of the issue. Additionally, no single entity has overarching responsibility and authority for the entire range of information management requirements (except for the fundamental responsibility and authority vested in the Secretary of Defense for all military matters). While remarkable progress is being made, it is inevitable that progress is, and will be, uneven. There is a danger that some aspects of the total information management requirement will be overlooked, not placed in proper priority, fall between the "seams" of the various initiatives, or fail to be integrated with other system elements. These kinds of failures are common to implementation of huge, complex initiatives. The 1998 Joint Strategy Review (JSR) Report addressed these concerns and provided specific recommendations, including the following:

> In the implementation of JV2010, we must focus on the development of a robust C4ISR infrastructure capable of providing sufficient on-demand, redundant, and seamless connectivity between forces at all levels...To preclude overwhelming man and machine, we must address the issue of information management (IM).[9]

There are a number of problems which must be addressed in order to achieve full success. One point to keep in mind is the requirement for interoperability with foreign militaries and non-military entities such as Non-Governmental Organizations. The CINC 21 ACTD proposal addresses this need, in part, by including the United Kingdom and Australia as potential partners in the ACTD. However, the interoperability requirement must extend far beyond our British and Australian allies. Joint Vision 2010 emphasizes the expectation for operating within coalitions as well as alliances. Interoperability is so important that one of the seven JSR major recommendations addressed multinational operations and interoperability at the tactical, operational, and strategic levels.[10] Together, documents which include Joint Vision 2010, the JSR, the CRD-IDM, and the CINC 21 ACTD provide a useful list of necessary attributes with which to assess the actual application of technology to information management requirements:

1. accurate
2. on-demand (often referred to as "timely")
3. prioritized
4. integrated
5. redundant (addresses reliability; not duplication)
6. seamless
7. interoperable at all levels
8. robust
9. distributed

How well are current and planned projects addressing these requirements at both the macro level (overall success at meeting requirement and relationship to other requirements) and micro level (specific attributes)? Before assessing efforts to achieve Joint Vision 2010 goals in information management, it is helpful to analyze the relevant information processes and procedures as presently applied.

THE INFORMATION CYCLE:

The military appears to lack a single, comprehensible doctrine for information management. Intelligence information, one type of information required by warfighters, offers a useful methodology for comprehending the entire process of information management. This concept is termed the Intelligence Cycle, which is explained in Joint Pub 2-0, Doctrine for Intelligence Support to Joint Operations.[11] The Intelligence Cycle consists of the following six phases: (1) Planning and Direction, (2) Collection, (3) Processing and Exploitation, (4) Analysis and Production, (5) Dissemination and Integration, and (6) Evaluation and Feedback. Let's examine each phase as it applies to the Information Cycle.

PLANNING AND DIRECTION PHASE:

The Combatant Commander is personally responsible for this phase, with key aspects of it usually assigned to his staff (particularly his J3, J5, and J6). The J3 and J5, with input from the remainder of the staff and as advised on technical matters by the J6, normally have the lead on determining information requirements. Of course the entire staff needs to participate in determining specific information requirements pertaining to intelligence, logistics, personnel, medical support, and other categories (depending on the operation). Even the best-designed information system will fail if the right information requirements are not identified. Additionally, it is essential that the requirements be prioritized based on their contributions to mission accomplishment. Information requirements potentially can be so vast that prioritization may actually drive many aspects of the system design, as will be discussed in detail later. In addition to establishing the information requirements, this phase determines the overall organization of the entire process, including a concept for implementation and resourcing its functions. While this phase sets the entire cycle in motion, it also must operate continuously to balance and optimize all phases of the cycle.

COLLECTION PHASE:

For the information cycle as well as the intelligence cycle, once the required information is identified, it must be collected. It is particularly important to note the current lack of emphasis on the means by which information is collected. The CINC 21 ACTD documentation implies that the required data already is "available"; that the challenge is in organizing, displaying, and disseminating it. As the CINC 21 ACTD Management Plan expresses the issue, "Where in the past the operations of a CINC were built around coping with information deficiencies, in the future the problem will be in dealing with information overload."[12] Similarly, the CRD-IDM, in defining the project scope, does not address information collection; attention is focused on dissemination as the critical factor in information management. This lack of attention to the collection phase of the cycle reflects two assumptions: (1) that collection currently is adequate, and (2) that collection is the purview of other entities (primarily by the intelligence community) and outside the scope of the ongoing information management initiatives. This potential problem will be discussed later in more detail.

PROCESSING AND EXPLOITATION PHASE:

The application of this phase to the information cycle is clear, although it differs somewhat in implementation from the intelligence cycle. In both instances, the data *as collected* usually cannot be delivered directly to the end user. It first must be routed to a processing station. Processing and exploitation requirements vary considerably depending on the source. In general, the data must be transformed from its raw form to some useable or understandable format. This may involve extracting the useable data, discarding the remainder, and organizing the data. This phase is critical in ensuring the information is both relevant and timely (ensuring the right information is captured, amongst everything that is collected, and efficiently exploited). The current efforts addressing information management tend

to focus on this phase as the *start* of the information management challenge, under the perhaps fallacious assumption that the requirements definition and collection phases are functioning properly.

ANALYSIS AND PRODUCTION PHASE:

This phase and the previous phase can overlap; more so in the information cycle than in the intelligence cycle. Analysis is essential to the intelligence cycle, whereas some warfighting data (for example, detection of an incoming missile) may require no analysis for it to be actionable information. In fact, the CRD-IDM treats this and the preceding phase as essentially one processing phase. Indeed, automation and application of artificial intelligence tends to blur the distinction between these two phases, as well as the dissemination phase, which follows.

DISSEMINATION AND INTEGRATION PHASE:

In the intelligence cycle, there is a clear distinction between the previous phases and the delivery of "finished intelligence" to the warfighter. It is the intelligence specialist's responsibility to ensure sufficiency in content, analysis, and format of presentation to meet the warfighter's needs, within the warfighter's decision cycle. To date, this end-to-end responsibility has not existed for the information cycle. Intelligence (by definition, knowledge of the adversary/potential adversaries and the battlespace) is only one category of information required by the warfighter. Thus there is a requirement for a holistic approach to information management--combining all the categories of information to best support the command decision-making function.

EVALUATION AND FEEDBACK PHASE:

Clearly the information cycle has the same need as the intelligence cycle for evaluation and feedback to ensure adjustment of the entire cycle to meet ongoing and emergent requirements. Considering the constantly changing nature of the warfighter's information needs as circumstances change, and the constantly changing opportunities for greater efficiency/speed/clarity/utility offered by emerging technology, modifications to the cycle likely will be required on a near-continuous basis. Therefore, flexibility must be designed into the cycle. The Evaluation and Feedback phase flows directly into the Planning and Direction phase. This completes the cycle and permits the entire process to continually adapt to users' requirements.

A NEW PARADIGM FOR INFORMATION MANAGEMENT?

The CRD-IDM also recognizes the lack of an overall concept for information management and offers an intriguing paradigm for organizing information requirements.

> We need a new way of characterizing and categorizing information to meet 21st Century Battlespace requirements. This characterization is based on the notion that there are two types of information used by the Joint Warfighter. These are "planning" and "survival" information.[13]

The CRD-IDM then provides definitions for "planning" and "survival" information. "'Planning' information is used as a basis for determining future action and is generally not time sensitive." In contrast, "'survival' information requires immediate action such as to attack the enemy, avoid being attacked, and/or to prevent fratricide. It is, therefore, extremely time sensitive."[14] There is merit to this concept, although there are also potential problems associated with it. As the CRD-IDM points out, "Current military information (C4) systems are designed to support the collection, analysis, storage, and distribution of non-time critical "planning" information not "survival" information."[15] This is only partially correct. The primary C4 system in use today, and the intended basis for future information management systems, is the Global Command and Control System (GCCS) with all its sub-components. GCCS is attempting to be the foundation for virtually all C4 warfighting management, to include "survival" as well as "planning" types of information. It may be a valid complaint that GCCS handles "planning" information better than "survival" information. However, it would be premature to dismiss GCCS as a failure at handling "survival" information. Several initiatives are underway to improve information flow, particularly timeliness, into GCCS. Nevertheless, the CRD-IDM proposal to differentiate between "planning" and "survival" information warrants consideration. As evident in the previous discussion of the Intelligence Cycle, there is no such *doctrinal* distinction within that cycle related to speed of delivery. Where timeliness is identified as critical and where technically possible, special paths have been established to expedite delivery of selected information to warfighters/decision makers, as the CRD-IDM notes with its mention of Signals Intelligence and Electronic Warfare. Otherwise, as a rule, the combatant commander's intelligence staff is responsible for identifying time-critical intelligence information and getting it where it needs to be to meet decision timelines. This, in fact, does take place. The USCINCPAC J2 makes a distinction between three categories of intelligence information, based on speed of delivery requirements. These divisions are "immediate", "perishable", and "reference".[16] Clearly, there is utility in differentiating between information types based on timeliness of delivery requirements. However, there is danger in dividing all information into just two categories (planning and survival) as proposed by the CRD-IDM, and then disseminating the information based solely on their categorization. This may limit the ability to tailor dissemination requirements to the situation. Moreover, the same information might be categorized differently depending on the level at which it will be used (strategic, operational, tactical) or proximity to the threat.

This proposed division of information into "survival" and "planning" categories drives the entire dissemination process, because the CRD-IDM proposes "Smart Push" of "survival information" (in real-time), and "User Pull" of "planning information" (as required).[17] Using a combination of "push" and pull" for dissemination is a sensible approach to information management. In fact, this principle of dual dissemination methods already is in use by the intelligence community. Joint Pub 2-0 specifies that, "...time-sensitive intelligence will be "pushed" to JFCs [Joint Force Commanders] and components by way of dedicated broadcasts ..." while "The "pull" concept results in a JFC requesting and receiving only intelligence relevant to the mission and current phase of the operation."[18] This dissemination scheme is

driven by Priority Intelligence Requirements (PIR), which are created during the Planning and Direction phase of the Intelligence Cycle. The PIR specify the delivery requirements (time, format, communications path, etc) for the intelligence. Consequently, doctrine is established (at least for the intelligence portion of the warfighter's information requirements) for getting "the right information to the right place at the right time", with the J2 specifically assigned responsibility. This concept can be directly applied to information management. If the Combatant Commander and his staff (principally the J5 and J3) perform their proper roles in defining their warfighting requirements (translated into Priority Information Requirements), the information system can be designed to meet their requirements, subject to resource, technology, and organization limitations.

The CRD-IDM addresses two of those three limitations: technology and organization. The information management paradigm proposed in CRD-IDM is particularly provocative because, if implemented, it may represent a significant change in how intelligence information is handled within the context of C4ISR. "C4 systems support to intelligence is normally limited to providing the communications interface and media required to move intelligence and related information. C4 systems support does not typically cover the collection and production of intelligence."[19] Although the CRD-IDM purports to deal with information *dissemination*, its proposed handling of some categories of "survival" information cannot be divorced from how certain intelligence information is "produced". One of the basic principles--virtually the *raison d'etre*--of intelligence is the analytical function.

> Processed and exploited information is converted into intelligence that satisfies the consumer's intelligence requirements. The conversion requires that information be appraised to determine its credibility, reliability, pertinence, and accuracy; integrated by selecting and combining information to form patterns; analyzed to review information to identify significant facts for subsequent interpretation; and interpreted to judge the significance of information in relation to the current body of knowledge.[20]

There are additional services provided by "processing". One procedure, used when appropriate, strips the data of evidence of how it was collected, protecting the source. This processing allows data to be provided to "consumers" who have a "need to know" at a lower security level, significantly increasing its accessibility. Care must be taken that emphasis on speeding information to consumers does not rob it of the "value added" by the elements of the Intelligence Cycle. The danger is that pursuing speed in delivering "survival" information to warfighters will be at the cost of ensuring its "credibility, reliability, pertinence, accuracy, integration, and interpretation"; all of which provide "added value" to the raw data. The CRD-IDM correctly recognizes the existence of the processing and analysis phases of the Intelligence Cycle. However, the CRD-IDM apparently does not recognize the necessity of the processing, analysis, and production steps. Instead, the CRD-IDM proposes,

> To provide the Joint Warfighter with critical "survival" information, selected intelligence system capabilities and processes must be reoriented and tailored to produce and disseminate time-critical "survival" information to specific Warfighters. Such information would include I&W of imminent attack, weapons targeting/retargeting information, and identification/classification of targets/forces about to be attacked by friendly forces (Combat ID). While such capabilities already exist to some extent in the areas of signals

intelligence (SIGINT) and EW, major improvements are needed, especially to support the targeting of smart weapons and the prevention of fratricide.[21]

The concept of automating intelligence information dissemination (or rather, increasing the automation of intelligence information dissemination, as it already is partially automated) must proceed very cautiously and with full participation by appropriate entities within the intelligence community. Indeed, there are significant potential hazards related to automating intelligence information flow. It is imperative that the information be accurate. The tradeoff between the fastest possible delivery of the information, and assurance of its fidelity, must be carefully considered and appropriate mechanisms emplaced for ensuring and/or verifying its accuracy. In the case of "Indications and Warning of imminent attack", which the CRD-IDM listed for inclusion in the "survival" category of information management, it should be noted that such information seldom is unambiguous. Certainly, the recognition and corresponding warning of imminent attack must be provided to the appropriate entities as fast as possible. However, the responsibility for such a function must be thoughtfully assigned, and the information management system so designed. Expediting information flow will not serve the warfighter if the information itself is erroneous, contradictory, or ambiguous.

SECURITY AND INTEROPERABILITY ISSUES

Information management for the military--particularly warfighting data--is inextricably entwined with security issues. Security-related restrictions on every aspect of information management work in direct conflict with the goals of efficiency, interoperability, and speed of delivery, to name a few. "Interoperability is defined as the ability of the IDM applications, processes, and services to facilitate the management of information dissemination across the entire Global Information Grid."[22] A chasm remains between the classified information commonly used by warfighters and resident in their C2 systems (at the SECRET and CONFIDENTIAL levels) and the compartmented information (usually intelligence information) which is needed at these same levels but is restricted due to national security concerns. A deeper chasm exists between information which is restricted to U.S. use only, and that readily available for sharing within an alliance or coalition. A true "multilevel" automated security capability has been identified as essential for years, but such a capability is not yet available. There are a number of reasons, ranging from organizational to technical, why multilevel security capability has not yet been achieved. Systemic problems include the lack of a single authority for security issues and the lack of a single program office or configuration manager for multilevel security (MLS) issues and efforts.[23] There is a recognized "lack of common standards, requirements, policies, and procedures for all security domains and for all MLS development"[24] Unfortunately, technical solutions to protecting the compartmented data within a heterogeneous system have not been developed in the civilian sector. The requirements for data security for sensitive compartmented information, and assurance of its access by only authorized entities, are extremely stringent, and somewhat unique to the intelligence community.

The CINC 21 ACTD is taking the only sensible approach, which is to begin the effort with the categories of information available to them at this time, with the recognition that the other categories will be incorporated when a multi-level security tool is accredited and available. In practice, that means the ACTD is limited to information available in the SECRET and lower security level domains, which severely restricts the potential for sharing the systems with non-U.S. personnel. This approach is preferable to delaying all efforts until multi-level security capability matures to the point of allowing all security levels to reside in one system. However, care should be taken to account for the future incorporation of multi-level security capability, in whatever form it may take. It would be counterproductive to invest in the numerous decision making tools, visual and audio display devices, information flow processes, etc with the intention of incorporating higher than SECRET inputs later, only to find that those portions of the future system-of-systems cannot be accredited at the higher security level. Very close interaction with the intelligence community and with managers of the compartmented portions of the operations community is essential if compartmented information is ever to be removed from "stovepipes" and fully incorporated into the operational C4 environment. Furthermore, security policies (including foreign disclosure policies) either need to be completely overhauled, or current policies accommodated by the information management efforts currently underway. It may be expedient, but unwise, to ignore those requirements in the hope that the challenges they present will either disappear or magically diminish in the future. Constant pressure needs to be brought to bear to influence security policy in the interests of interoperability goals. How and by whom this pressure can be brought to bear effectively are issues complicated by the lack of an overall authority for DoD-wide information management. The most logical entity under the current organizational structure is USJFCOM. However, with numerous commands working on aspects of the information management challenge, each command involved will need to be conscious of the numerous security and interoperability issues related to its piece of the puzzle. Due to the sheer complexity of security regulations and complicated technical aspects of the interoperability issues, the potential is particularly high that not all the information management issues will adequately address those requirements.

THE WAY AHEAD

The draft CRD-IDM is a visionary document, despite reservations about some aspects such as the proposed division of information into two ("planning" and "survival") categories. It contains excellent insights and offers intriguing solutions to information dissemination challenges. When finalized and implemented, it will provide a foundation for the direction of all information dissemination efforts. This will aid in standardizing information dissemination across all services and communities. While visionary, the CRD-IDM also takes a practical approach to finding solutions to information dissemination challenges. It builds on the existing foundation of the Global Command and Control System (GCCS); an imminently sensible approach. It takes an incremental developmental approach by setting achievable near-term objectives as well as long-term goals. The single largest fault of the CRD-IDM is inherent in its scope. By definition, it addresses only one aspect of the information management problem. It simply is not possible

to treat information dissemination separately from the rest of the information management cycle. It would have been preferable to first charter an overall Information Management Capstone Requirements Document. The information dissemination portion of the problem then could be addressed in detail. Establishing requirements for information dissemination without an overarching information management concept entails a risk of having those requirements drive other aspects of the overall information management development effort. The earlier discussion about potential problems related to the CRD-IDM's proposal to create "planning" and "survival" categories of information is a case in point. The proposed paradigm might very well be the ideal way to treat dissemination of information. However, it might not be considered ideal when overarching information management requirements are taken into account.

This does not mean the CRD-IDM effort should be cancelled or even shelved. It does mean that particular care must be taken to consider the implications of the CRD-IDM proposals within their larger context. Without an overarching concept, that consideration is extremely problematic. What will be the basis for determination of dissemination requirements within the overall information management design structure? USJFCOM, in finalizing the CRD-IDM, and the CJCS staff, in approving it, need to keep this issue in mind.

The CINC 21 ACTD, a concurrent project with a different focus, also has significant potential for achieving progress toward the goals defined in Joint Vision 2010.

> The envisioned residual of the CINC 21 ACTD, retained by the User-Sponsor, will be a fully integrated "next generation" command center capability, complete with decision support applications, visualization and display system hardware. It also will include distributed, virtual workspace software that can be used within the DII COE envelope of systems. Upon transition to GCCS, these segments will be available to all CINCs, Joint Forces and other users.[25]

The ACTD's focus is on the present and immediate future: what can be provided and implemented *now* to improve information management at the combatant commander's headquarters. Tools and components under development are using existing and emerging technology. These new tools and procedures will be tested and, if successful, validated through real world practical application. Spiral development will enable incremental improvements to the information management systems, in response to feedback and emerging technology opportunities. An inherently positive aspect of the ACTD is that it is experimental in nature and confined in scope. What "works" will be retained. What doesn't work will be a valuable, and relatively inexpensive, "lesson learned". The risk of failure is small in the sense that the commitment to any one design or organizational structure or system is not too large to be changed. This is particularly attractive in light of rapidly changing technology. It may not be desirable to make a large commitment to anything technology-based while the rate of change is so rapid. A flexible, modular construct is appealing in that it offers maximum potential for incorporating improvements as they become available. This approach should be supported and resourced.

The greatest remaining challenges are a result of the absence of a single controlling entity and single overarching concept for information management. Current efforts, however excellent they may be,

are piecemeal. The only logical entity to assume overall responsibility is the Joint Staff. The Joint Staff should consider applying the JROC and JWCA processes to the "big picture" information management issues. The Joint Staff also can assign the overall requirements formulation responsibility to a command such as USJFCOM, as it did the CRD-IDM. In fact, USJFCOM in its role as Joint Force Integrator already is assigned responsibility to ensure C4ISR interoperability across the Joint Forces.

Especially problematic aspects of information management include the security and interoperability issues. These issues need an approved overarching concept within which all the security and interoperability issues can be addressed. When an overall concept is created and agreed upon, security and interoperability strategies and requirements can be developed. At that point, application of the ACTD process may be very beneficial, particularly for interoperability development. Interoperability with foreign militaries is a particularly weak element of current efforts such as the CRD-IDM and the CINC 21 ACTD. It is not necessarily wrong to take the approach of addressing our own needs and goals first. It is, however, a mistake to disregard alliance and coalition interoperability issues in the system design phase. Obviously, these issues need to be resolved during peacetime. Achievement likely will reward us with a huge payback, even in peacetime, with its influence on the implementation of Theater Engagement Plans. Truly interoperable information systems could be a key aspect of allied and coalition exercises and serve to expedite communications on a routine basis. This can have a significant positive impact on our ability to "shape" the strategic environment. Lack of success could lead to catastrophic problems in the event of a crisis requiring coalition operations, as well as creating problems and frustration during peacetime operations and training. We simply cannot afford to neglect these issues.

RECOMMENDATIONS

The single most important and most urgent need is for the creation of a single, DoD-wide overall doctrinal concept for information management. This concept must take into account all the necessary attributes, properly balancing accuracy, timeliness, interoperability, and other essential requirements. It must be realistic with regard to problematic areas such as security. It must provide a basic roadmap from which various aspects of the challenge can be worked on, and to which separate efforts will all relate. This concept must be backed by the authority of the CJCS, in order to require all development efforts to comply with the common vision. USJFCOM is the likely candidate for leading the coordination effort. The responsible agency (CJCS staff or a designee such as USJFCOM) must aggressively work the common problem areas such as security and interoperability. That responsibility should be expanded for other aspects of information management, as information management requirements and issues are more likely to be shared by all the services and combatant commands than to be unique. CJCS needs to get further out in front on information management requirements issues than it is now, in order to drive the acquisition, fielding, and training issues which the Services will implement.

In designing the overarching information management concept, it should be viewed as a cycle, similar to the Intelligence Cycle. This construct is very useful in assuring that all aspects of the entire process are properly related to each other and that the entire process continuously meets the needs of

the end-users. The highest possible degree of flexibility and responsiveness needs to be built into the overall concept and each component process. The one certainty is continued uncertainty, due to the rapid rate of technological change and the highly dynamic world environment and its changing demands on the military. Joint Vision 2010 is a goal; the foundation on which to build all future requirements and acquisition -- until the next vision emerges. Information management must be addressed in that context -- working as rapidly and efficiently as possible toward that vision, but poised to adjust to the requirements inherent in the next vision. With implementation of the proposed recommendations, the current efforts can be directed toward achievement of an effective information management environment. This information management environment can, in turn, enable true information superiority and genuine interoperability--hallmarks of Joint Vision 2010.

WORD COUNT = 5512

ENDNOTES

[1] Joint Chiefs of Staff, Joint Vision Implementation Master Plan, CJCSI 3010.02 (Washington, D.C.: U.S. Joint Chiefs of Staff, 9 December 1998), 1.

[2] J6, Joint Forces Command, Capstone Requirements Document for Information Dissemination Management, draft working paper (Norfolk, VA: U.S. Joint Forces Command, 18 December 1999), 7.

[3] Joint Chiefs of Staff, Joint Vision 2010 (Washington, D.C.: U.S. Joint Chiefs of Staff, July 1996), 14.

[4] Michael J. Vickers, "The Revolution in Military Affairs and Military Capabilities," in War in the Information Age, ed. Robert L. Pfaltgraff, Jr. and Richard H. Schultz, Jr. (Herndon, VA: Brassey's, 1997), 33.

[5] Vice Chairman, Joint Chiefs of Staff, JROC Memo 069-99, memorandum for U.S. Joint Forces Command, Washington, D.C., 8 July 1999.

[6] J6, Joint Forces Command, Capstone Requirements Document for Information Dissemination Management, draft working paper, 4.

[7] J62, Pacific Command, "FY2000 ACTD Proposal," memorandum for Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts, Camp Smith, HI, 2 July 1999.

[8] Joint Chiefs of Staff, Joint Vision 2010, 14.

[9] Joint Chiefs of Staff, 1998 Joint Strategy Review Report (Washington, D.C.: U.S. Joint Chiefs of Staff, 4 September 1998), 2.

[10] Ibid., 3.

[11] Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, Joint Pub 2-0 (Washington, D.C.: U.S. Joint Chiefs of Staff, 13 July 1998), II-1-2.

[12] J62, Pacific Command, "CINC 21 Advanced Concept Technology Demonstration Management Plan," memorandum for Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts, Camp Smith, HI, 21 October 1999.

[13] J6, Joint Forces Command, Capstone Requirements Document for Information Dissemination Management, draft working paper, 7.

[14] Ibid., 5.

[15] Ibid., 11.

[16] Mike Shimamoto, "PACOM Coalition Architecture Implementations for Theater and Ad Hoc Operations," briefing graphics, Camp Smith, HI, U.S. Pacific Command J2, 1 February 2000.

[17] J6, Joint Forces Command, Capstone Requirements Document for Information Dissemination Management, draft working paper, 17.

[18]Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, IV-12.

[19] Ibid., IV-1.

[20] Ibid., III-8.

[21]J6, Joint Forces Command, Capstone Requirements Document for Information Dissemination Management, draft working paper, 14-15.

[22] Ibid., 23.

[23]Mike Shimamoto, "PACOM Coalition Architecture Implementations for Theater and Ad Hoc Operations," briefing graphics.

[24]Mike Shimamoto, "Information Sharing Initiatives," briefing graphics, Camp Smith, HI, U.S. Pacific Command J2, 7 December 1998.

[25]J62, Pacific Command, "FY2000 ACTD Proposal," 7.

BIBLIOGRAPHY

Shimamoto, Mike. "Information Sharing Initiatives." Briefing graphics. Camp Smith, HI: U.S. Pacific Command J2, 7 December 1998.

_____. "PACOM Coalition Architecture Implementations for Theater and Ad Hoc Operations." Briefing graphics. Camp Smith, HI: U.S. Pacific Command J2, 1 February 2000.

U.S. Joint Chiefs of Staff. 1998 Joint Strategy Review Report. Washington, D.C.: U.S. Joint Chiefs of Staff, 4 September 1998.

_____. Doctrine for Intelligence Support to Joint Operations. Joint Pub 2-0. Washington, D.C.: U.S. Joint Chiefs of Staff, 13 July 1998.

_____. Joint Vision 2010. Washington, D.C.: U.S. Joint Chiefs of Staff, July 1996.

_____. Joint Vision Implementation Master Plan. CJCSI 3010.02. Washington, D.C.: U.S. Joint Chiefs of Staff, 9 December 1998.

U.S. Joint Forces Command, J6. Capstone Requirements Document for Information Dissemination Management. Draft Working Paper. Norfolk, VA: U.S. Joint Forces Command, 18 December 1999.

U.S. Pacific Command, J62. "CINC 21 Advanced Concept Technology Demonstration Management Plan." Memorandum for Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts. Camp Smith, HI, 21 October 1999.

_____. "FY 2000 ACTD Proposal." Memorandum for Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts. Camp Smith, HI, 2 July 1999.

Vice Chairman, U.S. Joint Chiefs of Staff. Joint Requirements Oversight Council Memo 069-99. Washington, D.C.: U.S. Joint Chiefs of Staff, 8 July 1999.

Vickers, Michael J. "The Revolution in Military Affairs and Military Capabilities." In War in the Information Age, ed. Robert L. Pfaltgraff, Jr. and Richard H. Schultz, Jr., 29-46. Herndon, VA: Brassey's, 1997.